Providing the Foundation for Security Certification Within U.S. Government Civil Agencies Integrated Communications, Navigation, and Surveillance (ICNS)

Contacts:

Beryl Hosack • 301-921-3440 • bhosack@csc.com

Joe Guirreri• 703-279-3588 • Jguirrer@csc.com

ICNS Conference

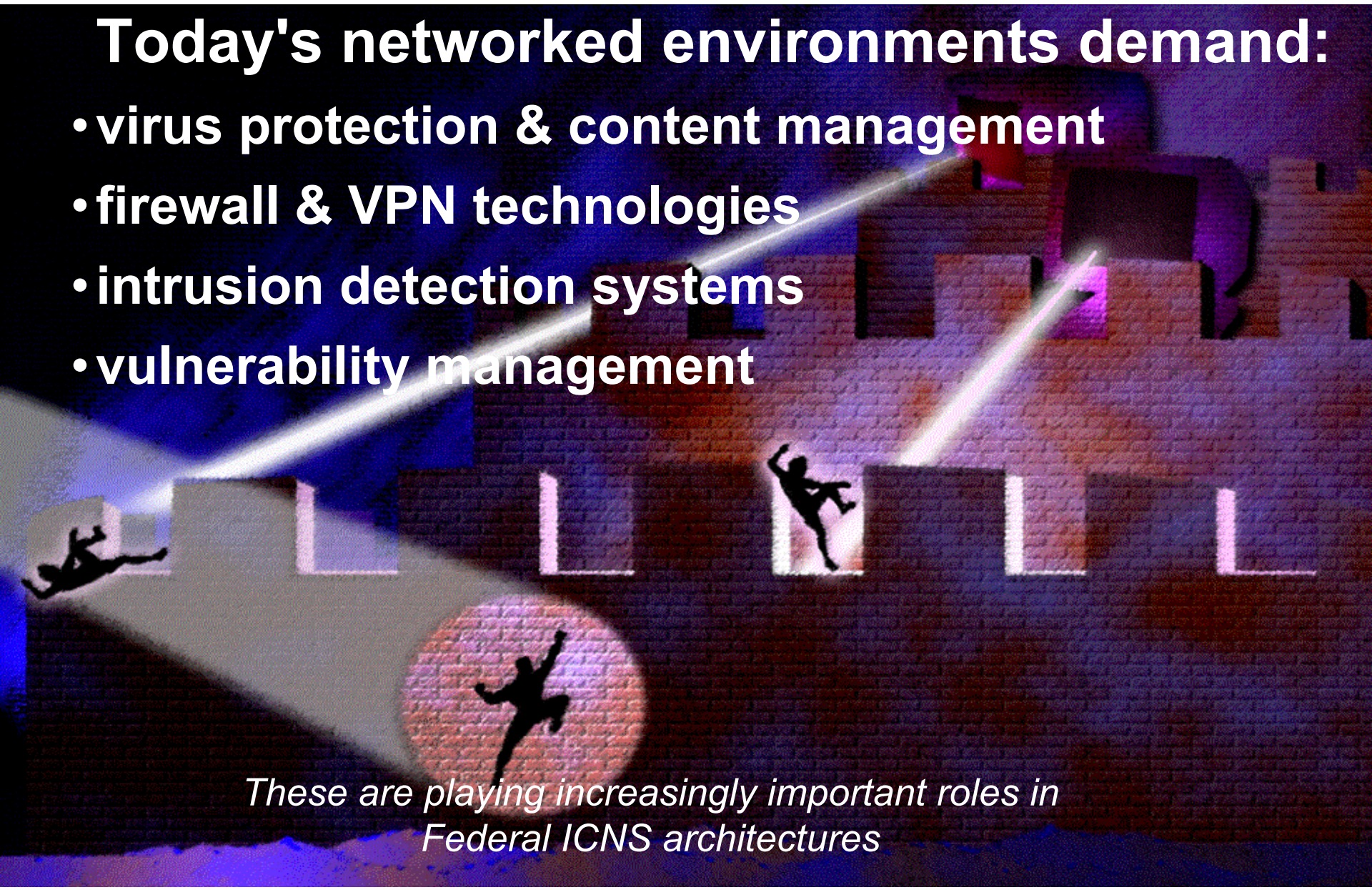
Annapolis Md.

May 2003

Introduction

Today's networked environments demand:

- virus protection & content management
- firewall & VPN technologies
- intrusion detection systems
- vulnerability management



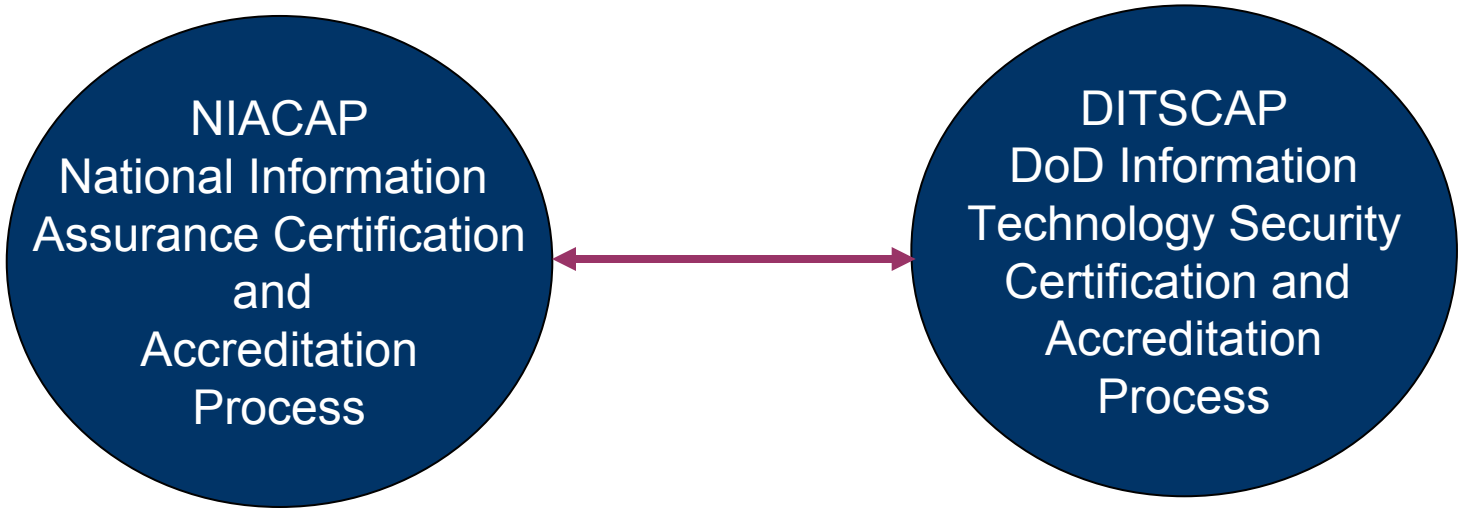
These are playing increasingly important roles in Federal ICNS architectures

Federal Security Certification: A Uniform Integrated Approach

- Open Federal Recommendations Identify Security Problems as Widespread
- "Horne Committee Report" & U.S. General Accounting Office
  - Homeland Security Department will inherit many IT management problems of it's component agencies
- Federal Civil agency Chief Information Officers increasingly asked to:
  - identify significant IT system vulnerabilities
  - establish performance goals for eliminating these weaknesses
  - quarterly evaluations of performance goals
- Post "September 11" requirements to bolster IT security services a key driver for security certification

U.S. Federal Civil agencies rapidly moving to uniform security certification of enterprise architectures and the configured IT applications residing within them

Federal Approach to Security Certification



- **Both processes standardize activities leading to successful Accreditation**
- **Combining these programs allows the US to secure and protect ICNS infrastructures**

Standardizing the processes minimize risks associated with nonstandard security implementations across shared infrastructure and end systems

Federal Security Certification Process: A Phased Approach

- **Phase 1, Definition:**
  - includes activities to document system mission, environment & architecture
  - identifies the threat(s)
  - defines levels of effort
  - identifies the certification authority (CA) & designated approving authority (DAA)
  - documents necessary security requirements for Certification & Accreditation

Phase 1 culminates with a documented agreement between the program manager, the DAA & CA, & the user representative of approach/results of phase 1 activities

Federal Security Certification Process: A Phased Approach (continued)

- **Phase 2, Verification:**
  - **perform activities which verify system compliance with (previously agreed) security requirements**
    - **for each life cycle development activity there is a corresponding set of security activities verifying compliance with security requirements**
  - **evaluate vulnerabilities**

Phase 2 culminates with verification that security requirements are met

Federal Security Certification Process: A Phased Approach (continued)

- **Phase 3, Validation:**
  - **activities to evaluate the fully integrated system**
  - **activities to validate system operation in a specified computing environment with an acceptable level of residual risk**

Validation culminates in an approval to operate

Federal Security Certification Process: A Phased Approach (continued)

- **Phase 4, Post Accreditation:**
  - monitor system management and operation
  - ensure an acceptable level of residual risk is preserved
  - conduct periodic reviews
    - security management
    - change management
    - compliance validation

These four phases of security certification are tailored and supplemented depending on the needs of the individual Federal department or agency

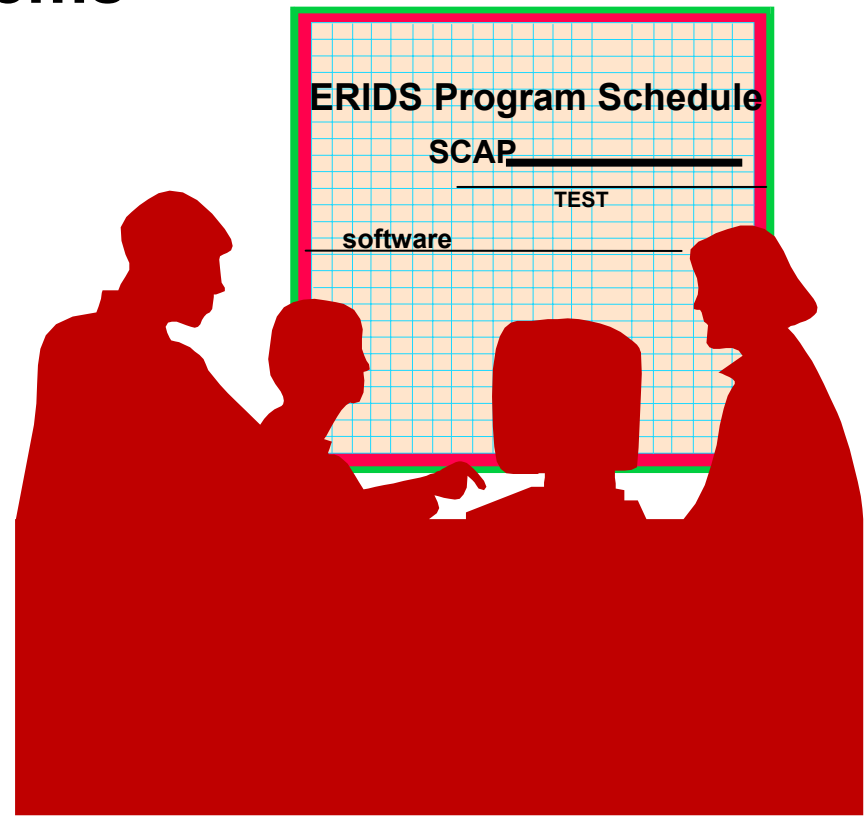
The FAA Information System Security Program

- **Presidential Decision Directive 63 (PDD-63), Protecting America's Critical Infrastructures**
  - **called on the FAA to protect the National Airspace System (NAS) from cyber attack**
- **FAA Order 1370.82 " Information Systems Security Program" developed in response to PDD-63**
  - **requires "all NAS, mission support and administrative systems (be) appropriately secured" before reaching operational status in the field**
  - **Security Certification and Authorization Package (SCAP): the documents showing proof of appropriate security**
    - **physical security, personnel security & computer security**

Locate details on :FAA home page instructions & guidelines, AUA Quarterly, December 2002

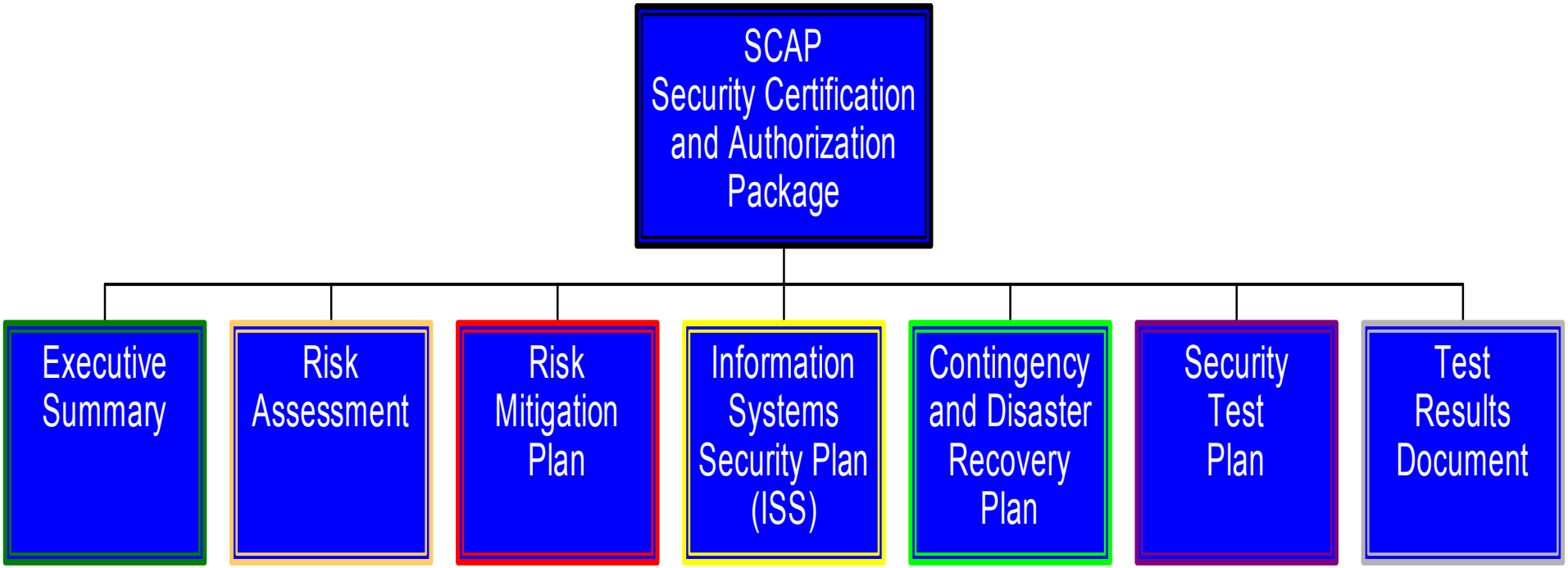
SCAP Process: A necessary Step in Fielding FAA Systems

- Process can take from a few weeks to months
- Need exists to budget time into the program schedule
- Without an approved SCAP, systems can not go to operational status in the field



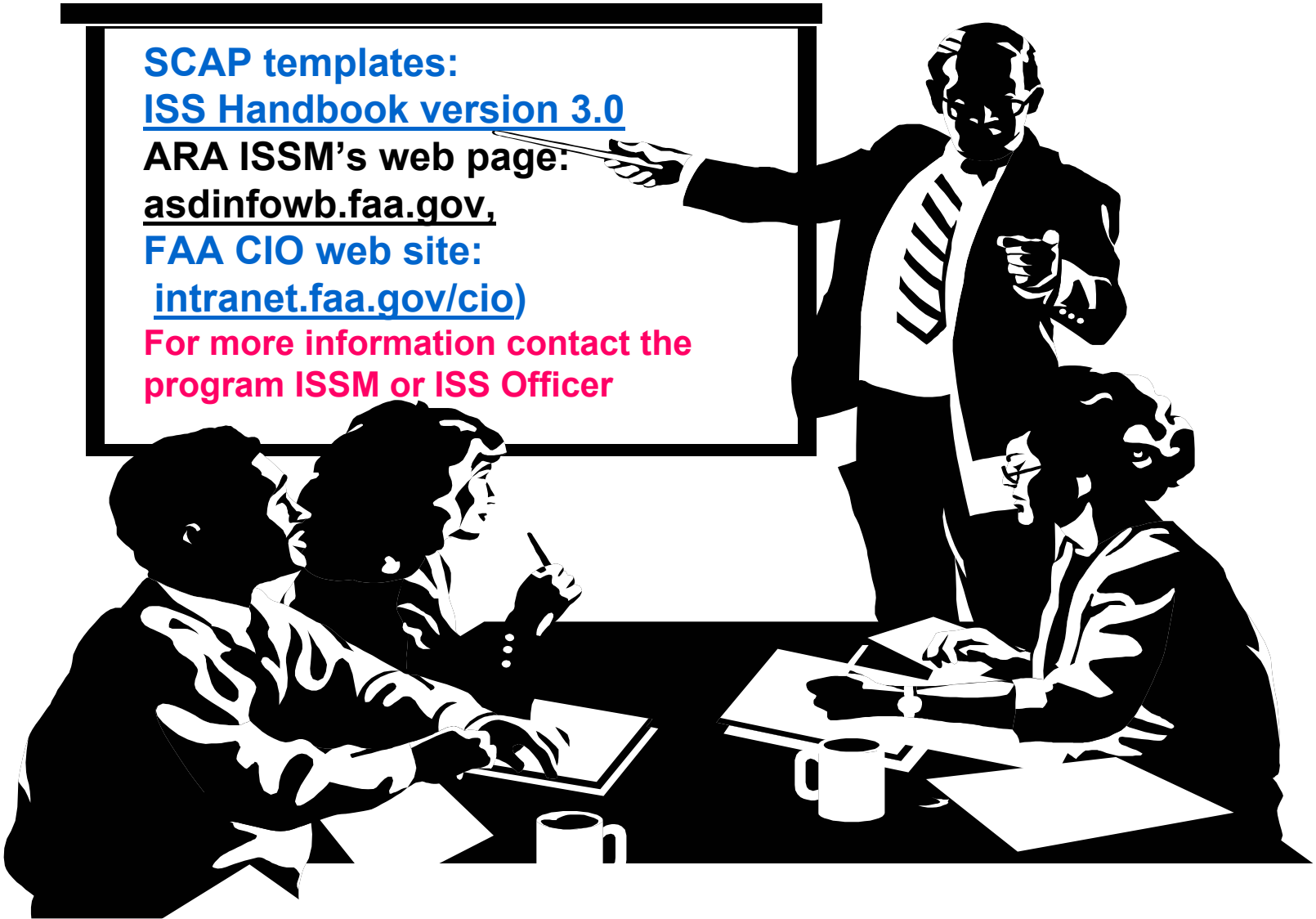
SCAPS give the FAA assurance that systems being fielded can be trusted to protect both the fielded system as well as the NAS & data processed within

FAA SCAP: An Excellent Example of the C&A Process



The Integrated Product team (IPT) must develop a SCAP & get it approved before a system can be approved for field operations

What Resources are Available to build a SCAP?



Key Steps for FAA Security Certification

- Team meets with project Information System Security Manager (ISSM) & AOP-500 (for NAS systems)
  - discuss the system
    - information gathering to assist in SCAP document development
    - plan for routine meetings during development/testing
    - resolution of any issues identified during the risk assessment
  - documentation development schedule
  - approval process
- Early on, project team briefs Office of Information Systems Security (AIS), NAS Operations Program (AOP), the ISSM & other involved organizations
  - helps accelerate the security certification process & clarifies the security approach ***at the beginning of the program***

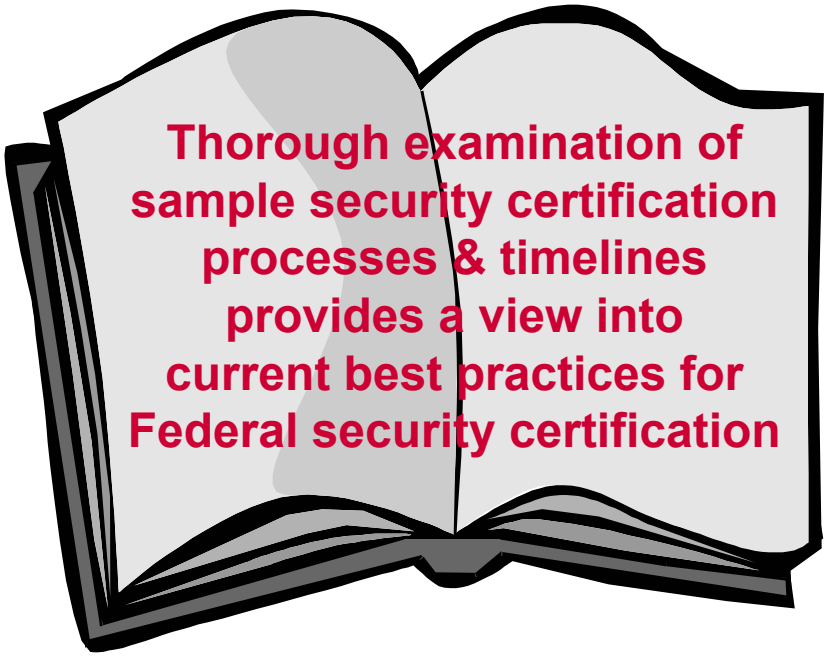
Early resolution of security issues results in clearing any misconceptions and developing meaningful security documentation

Key Steps for FAA Security Certification (continued)

- ISSO reviews the SCAP for compliance with FAA order 1370.82
- Following ISSO approval, Associate ISSM reviews package
  - any issues resulting from review are resolved by the IPT
- Associate ISSM then makes a recommendation and, if satisfied with the SCAP package, signs the certificate
- Package passed to ISSM
  - reviews document with their team, providing comments to the IPT
  - with resolution of issues by the IPT, package is signed by the ISSM and returned to the IPT
- IPT takes SCAP package to AOP-500 for review of "technical completeness"
- With resolution by IPT of AOP-500 comments, AOP-500 makes a recommendation to the Designate Approving Authority

Only with the signature of the Designated Approving Authority is the system authorized to operate in the NAS

Security Certification for ICNS can't be a "One Size Fits All" Approach



- ICNS systems have embedded integration complexities
  - determining necessary security services & security certification mechanisms prior to deployment & operational use
- Standards & guidelines for security certification exist
  - tend to be applied to each department as needed
- Security certification within the Federal government includes:
  - risk assessment, security plan, security test plan & results, contingency planning and a risk mitigation plan & schedule

Using a "best practices " approach, maximum benefit to Integrated Communications, Navigation & Surveillance systems within & beyond U.S. Federal Civil agencies can be achieved